

EXHIBIT B

Alight - Report of Investigation

Type of Incident:	Identity Theft, Theft	Date of Report:	9/18/20
Internal Case #:	██████████	Date of Incident:	1/29/20 – 3/17/20
Company Name:	Colgate-Palmolive	Impacted plan(s):	DC
Customer Name:	Disberry, Paula	ARC Investigator:	Jeff Barry

Executive Summary

Brief Description of Incident:

On 1/29/20, a bad actor contacted the Customer Care Center and impersonated the customer. During the interaction, the caller provided the customer's full name, last 4 of SSN, date of birth, and current address on file. The caller requested a Phone PIN reset. A temporary Phone PIN was sent to the address on file in South Africa and, about three weeks later, was entered into Alight's Automated Phone System and a permanent Phone PIN was chosen.

Over the next several months, the bad actor continued to impersonate the customer via calls to the Customer Care Center and the website. The changes processed included adding an email address, international telephone number, bank account for direct deposit, and a new permanent address in Las Vegas, NV. In each instance, calls to the Customer Care Center were properly secured. Web sessions were properly authenticated and occurred from IP addresses in South Africa. There was no evidence a user accessed any other accounts via outbound Single-Sign-On.

On 3/17/20, the bad actor contacted the Customer Care Center, secured the call by Phone PIN, and requested a total distribution from the 401k to be paid by check to the address on file in Las Vegas, NV. This address was added to the account earlier that same day, via the web. The distribution was processed for \$751,430.53 gross (\$601,144.42 net). A check was sent for the net amount and cashed on 3/27/20.

The suspected 401k fraud was reported to Alight by Colgate-Palmolive on 9/14/20. Contact information on file for the customer is presumed connected to the bad actor. As such, Alight requested contact information from Colgate-Palmolive for customer outreach. Based on the investigation results, there is sufficient evidence to conclude the customer appears to have been the victim of identity theft and theft of 401k funds. A summary of the investigation and talking points about identity theft and 401k theft will be provided to the customer. The customer will be encouraged to contact law enforcement to have the incident investigated and Alight will fully cooperate. Refer to the Narrative of Investigation for detailed information.

Investigation

Narrative of Investigation:

For background, this customer is a 52-year-old former employee who lives in Cape Town, South Africa. The customer last worked for Colgate-Palmolive in 2004.

On 9/14/20 at 6:00pm EST, a representative from Colgate-Palmolive contacted Alight by email and reported they believed a customer had a fraudulent 401k distribution. The customer was identified as Paula Disberry and the distribution was reported to have occurred on 3/17/20.

On the morning of 9/15/20, the incident was first evaluated by Alight's Fraud Protection Team. It was noted a total distribution occurred from the customer's account on 3/17/20 for \$751,430.53 gross (\$601,144.42 net) via a fully secured call to the Customer Care Center. The proceeds were sent by check payable to the customer at an address on file in Las Vegas, NV.

A freeze was placed on the account by Alight's Fraud Protection Team. The incident was then escalated to Alight's Investigations Team and the Alight Response Center on the evening of 9/15/20 at which time the investigation began. On 9/16/20, Alight contacted Colgate-Palmolive by email and requested current contact information for the customer.

An investigation was conducted. All relevant telephone calls into the Customer Care Center, which are summarized below, were recorded, and preserved in the investigation case file. Data from all web activity summarized below were also preserved and reviewed. The following events are presented in chronological order.

On 1/29/20 at 1:20pm CST, a caller contacted the Customer Care Center and identified as the customer. The caller said she wanted to change information in her account. The caller said she did not have the Phone PIN. When asked, the caller correctly provided the customer's name, last 4 of the customer's SSN, date of birth, and mailing address on file at [REDACTED] Cape Town, South Africa (on file since 10/31/17). The caller was told a Temporary Phone PIN would be sent to the address on file, located in South Africa. The call ended.

On 1/29/20, a Phone PIN Reset (Temporary Phone PIN) was sent to the customer by postal mail to [REDACTED] Capetown, South Africa.

On 2/24/20 at 12:07pm CST, a caller connected to Alight's Automated Phone System, correctly entered the Temporary Phone PIN (sent earlier by postal mail) and chose a Permanent Phone PIN. The call then connected to the Customer Care Center and the caller identified as the customer. This caller sounded like the previous caller from 1/29/20. The caller said she wanted to update information in

her account. The caller provided an email address of [REDACTED]¹. The caller provided a new international home telephone number ending in #0169 and requested it be added to her account. The caller was told a ticket would be created to add the international telephone number. The caller asked about logging into the website and was provided instructions. The caller said she misplaced her User ID and Password and was told those could be requested on the website. The call ended.

On 2/24/20, an Access Information Change Notice was sent to the customer by postal mail to [REDACTED] Capetown, South Africa.

On 2/24/20 at 12:11pm CST, records show the international phone change ticket was completed and an international home telephone number was added to the customer's account for a number ending in #0169. This removed the previous home telephone number, ending in #8201, which had been on file since 10/31/17.

On 2/28/20 at 1:45pm CST, the customer's account was attempted to be accessed via the web from an IP address assigned to [REDACTED] in Johannesburg, South Africa ([REDACTED]). The user chose the forgot password option and then entered the last 4 of the customer's SSN and date of birth. The user was challenged, chose to receive a one-time-code by text, and did not successfully complete the challenge. At the time, there was no personal email address on file. There was no successful access to the account.

On 2/28/20 at 1:58pm CST, a caller contacted the Customer Care Center and identified as the customer. The call was fully secured by Phone PIN entry in the Alight's Automated Phone System (Phone PIN created 2/24/20). This caller sounded like the previous callers. The caller said she wanted to activate an email address for her "online banking." The caller said she tried to log on from the website but received an error indicating she did not have an email address on file. The caller provided an email address of [REDACTED] and requested it be added. There was no personal email on file prior to this. The call ended.

On 2/28/20 at 1:59pm CST, records show an email address of [REDACTED] was added to the account as the personal email. There was no personal email address on file prior to this.

On 2/28/20, a Contact Information Change Confirmation email was sent to [REDACTED].

¹ While the caller provided an email address and requested her account be updated with the information, there was no evidence the information was entered into the customer's account on this date.

On 2/28/20, an Access Information Change Notice was sent to the customer by postal mail to [REDACTED] Capetown, South Africa and by email to [REDACTED].

On 2/28/20 at 2:04pm CST, the customer's account was attempted to be accessed via the web from an IP address assigned to [REDACTED] in Johannesburg, South Africa ([REDACTED]). The user chose the forgot password option and then entered the last 4 of the customer's SSN and date of birth. The user was challenged, chose to receive a one-time-code by email, did not successfully complete the challenge, and requested a password reset by email. There was no successful access to the account.

On 2/28/20 at 2:25pm CST, the customer's account was attempted to be accessed via the web from an IP address assigned to [REDACTED] in Johannesburg, South Africa ([REDACTED]). The user chose the forgot password option and then entered the last 4 of the customer's SSN and date of birth. The user was challenged, chose to receive a one-time-code by email, did not successfully complete the challenge, and requested a password reset by email. There was no successful access to the account.

On 2/28/20 at 3:13pm CST, the customer's account was accessed via the web from an IP address assigned to [REDACTED] in Johannesburg, South Africa ([REDACTED]). The user entered the last 4 of the customer's SSN and date of birth and a temporary password that had been sent by email to [REDACTED]. Once the information was correctly entered, the user chose a User ID, Password, and Security Questions/Answers. Once in the account, the user viewed the Savings Summary, Beneficiaries, Contribution Details, and Summary Plan Description web pages. No other changes were made to the account.

On 2/28/20, a Password Reset Confirmation Notice was sent to the customer by postal mail to [REDACTED] Capetown, South Africa.

On 2/28/20, an Access Information Change Notices were sent to the customer by email and postal mail to [REDACTED] Capetown, South Africa and by email to [REDACTED].

On 3/9/20 at 1:47pm CST, the customer's account was accessed via the web from an IP address assigned to [REDACTED] in Johannesburg, South Africa ([REDACTED]). The user entered the User ID/Password (created 2/28/20) and was challenged. The user elected to answer the Security Questions on file (also created 2/28/20) and successfully completed them. Once in the account, the user viewed the Personal Information, Financial Institution, Beneficiaries, and Savings Summary web pages. During the session, at 1:59pm CST, the user added a direct deposit for Bank of America for an account ending in # [REDACTED], Routing # [REDACTED]. During the session,

the user modeled a 401k distribution, but received an error and did not complete it². No other account changes occurred during the session.

On 3/9/20, a Contact Information Change Confirmation email was sent to [REDACTED].

On 3/9/20 at 2:46pm CST, a caller contacted the Customer Care Center and identified as the customer. The call was fully secured by Phone PIN entry in Alight's Automated Phone System (Phone PIN created 2/24/20). This caller sounded like the previous callers. The caller said she was having trouble with her "online banking" and later, when questioned, clarified she meant the 401k account. The caller said she was able to login to the account but was unable to make a "deposit." The caller was told the 401k department did not accept deposits. The caller said she needed help regarding how to make payments and further explained she wanted to make a withdrawal. Assistance was provided. The caller logged into the website and was walked through the steps to take a distribution. The caller said she was prompted on the website where to receive a check for the withdrawal. The caller said she was not given a direct deposit option. The caller was told a direct deposit had to be on file for seven days and one had just been entered for her account earlier in the day³. The caller asked if there were any other options for a distribution (other than a check) and was told no. The caller said she would wait the seven days and then attempt the distribution. The call ended.

On 3/16/20 at 5:35am CST, the customer's account was accessed via the web from an IP address assigned to [REDACTED] in Johannesburg, South Africa ([REDACTED]). The user entered the User ID and Password (created 2/28/20). The user viewed the Personal Information, Financial Institution, Beneficiaries, and Savings Summary web pages. No changes were made, but the activity described in the phone call summarized above was observed to have occurred at the same time as the call (including modeling a 401k distribution, but not completing the process).

On 3/17/20 at 10:58am, the customer's account was accessed via the web from an IP address assigned to [REDACTED] in Johannesburg, South Africa ([REDACTED]). The user entered the User ID and Password (created 2/28/20). At 10:58:50am CST, a total distribution was requested, and stepped-up authentication occurred. The user elected to receive a one-time-code to [REDACTED] (on file since 2/28/20). The one-time-code was sent and correctly entered; however, the distribution was not allowed to process by check to an address outside of the United States. At 11:03am CDT, during the same web session, the user changed

² The user received a page error (CsErr200DfltCrtcOpen) which is suspected as the user was attempting a distribution to be paid by direct deposit, which was not an available option at the time.

³ This statement by the Customer Service Representative, regarding a 7-day waiting period, was inaccurate as this was not in place at the time.

the permanent address from an address in South Africa (on file since 10/31/17) to an address in Las Vegas, NV. No other changes occurred.

There was an additional successful login to the customer's account on 3/17/20 at 1:49pm CST from an IP address assigned to [REDACTED] in Johannesburg, South Africa ([REDACTED]). The user entered the User ID and Password (created 2/28/20) and was challenged. The user elected to receive a one-time-code by email to [REDACTED] (on file since 2/28/20). The one-time-code was entered correctly, access was granted, and no changes were made to the account. The user viewed the Financial Institution and Savings Summary web pages. No changes were made to the account.


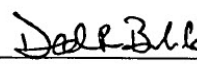
On 3/17/20, a Contact Information Change Confirmation email was sent to [REDACTED].

The same day, at 2:10pm CST, a caller contacted the Customer Care Center and identified as the customer. The call was fully secured by Phone PIN entry in Alight's Automated Phone System (created 2/24/20). This caller sounded like the previous callers. The caller requested a total distribution from the 401k and said she had attempted it by direct deposit. The caller was told Colgate-Palmolive did not offer distributions by direct deposit. The caller reaffirmed she wanted to take a total distribution. When asked, the caller provided the customer's full name. Initially, when asked for the address on file, the caller provided the prior address on file (located in South Africa). The caller was told the address she provided was incorrect and the current address on file was located in the United States. The caller then correctly provided the Las Vegas, NV address (added to the account earlier in the day). The caller confirmed she was logged into the account at the time of the call. She was told she would be logged off in order for the Customer Care Representative to conduct the distribution transaction. The caller was provided with the 401k balance and given four options for withdrawal. The caller chose the first option and requested the total distribution where stock funds would be taken as cash. The caller was told the distribution would be processed and sent by check to the address in Las Vegas, NV. The total distribution from the 401k was processed for \$751,430.53 gross (\$601,144.42 net) and the proceeds were sent by check in the customer's name to the address in Las Vegas, NV.

On 3/17/20, a Confirmation of Payment Notice was sent by postal mail to the address in Las Vegas, NV.

On 3/17/20, a DC Payment Confirmation was sent by email to [REDACTED].

A copy of the endorsed, cashed check was obtained from the Trust, BNY Mellon. The back of the check shows it was cashed on 3/27/20 (see below).

 BNY MELLON P.O. Box 569 Pittsburgh, PA 15230-0569		COLGATE-PALMOLIVE SAVINGS & INVESTMENT PLAN CL601T 8-26/430	
NOT VALID BEFORE OR 180 DAYS AFTER 03/20/2020		CHECK DATE	CHECK NUMBER
PAY SIX HUNDRED ONE THOUSAND ONE HUNDRED FORTY FOUR DOLLARS & 42 CENTS			
TO THE ORDER OF:	PAULA DISBERRY 1101 DUMONT BLVDW30 LAS VEGAS, NV 89169-4236	\$***601,144.42	
THE BANK OF NEW YORK MELLON PITTSBURGH, PENNSYLVANIA		 AUTHORIZED AGENT	

⑈0014375908⑈ ⑈043000261⑈ 900⑈8736⑈

 		ENCLOSE HERE  THIS AREA IS RESERVED FOR THE PROXY STAMP ON THE reverse side of this instrument. In the event the proxy is to be kept, the stamp must be retained attached. <input type="checkbox"/> CHECK HERE IF MOBILE DEPOSIT DO NOT WRITE, STAMP OR SIGN BELOW THIS LINE
--	--	--

On 5/8/20 at 9:38am CST, a caller contacted the Customer Care Center and identified as the customer. This caller did not sound like the previous callers from 1/29/20 – 3/17/20. The caller provided the customer's name and last 4 of SSN. This caller was difficult to understand due to the poor audio connection on the caller's end. The caller asked the balance of her savings account. The caller was asked to verify the address on the account and provided the prior address on file in South Africa. The caller did not provide the current address on file Las Vegas, NV. The caller then provided an address in Frisco, TX which also did not match the current address on file in Las Vegas, NV. The caller was unable to authenticate the call. The caller was told there was a phone number ending in #5110 on the account. The caller said she did not have access to that number to receive a one-time-code. A one-time-code was sent to the email address on file and the caller said she never received the one-time-code and was having connectivity issues. The caller was also unable to confirm the email address on file. The call disconnected a short time later. No account information was provided.

Additional phone calls were received in the Customer Care Center on 5/15/20, 5/18/20, 5/19/20, 6/4/20, 6/8/20, and 7/28/20 but none of these calls were properly secured. The callers did not sound like the previous callers from 1/29/20 – 3/17/20. In each instance, the caller did not have a Phone PIN or access to receive a one-time-code and was therefore unable to secure the calls or obtain any account information.

Additional login attempts were made to the account, via the web, from IP addresses in South Africa on 5/8/20, 5/15/20, 5/17/20, 5/19/20, 5/27/20, 6/8/20, 7/17/20, and 7/22/20. None of these attempts were successful.

We reviewed all web activity for this customer's account and found no evidence of any outbound Single-Sign-On sessions to any third-party websites.

We conducted a search to determine if other Colgate customers were affected by the IP addresses, email address, international telephone number, and direct deposit bank account identified in this investigation. The result showed no new matches. We conducted a search of internal colleagues who accessed the customer's account in CS Pro. The results revealed no suspicious internal activity.

We preserved all of the call logs, transaction data, and recorded telephone calls in the investigative case file. There does not appear to have been any failure in any Alight technical process or protocols which led to the processing of the events.

Customer(s) impacted

Name	Person identifier	Funds withdrawn?	Active Employee?
Disberry, Paula	[REDACTED]	Yes <input checked="" type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>

Investigation Research

What IP addresses were used to access the impacted accounts?	[REDACTED]	
Was there any suspicious activity discovered on Alight internal systems?	Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>	If yes, provide details:
If a bank account was changed on the impacted account(s), was this suspicious bank account on file for any other customers?	Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>	If yes, provide details:
If there were suspicious calls to the Alight Customer Care Center related to the impacted account(s), have the telephone number(s) used appeared on any calls for other customer accounts?	Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>	If yes, provide details:
If the email address changed on the impacted account(s), was this suspicious address on file for any other customers?	Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>	If yes, provide details:
Did any of the IP addresses access any other employee accounts?	Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>	If yes, provide details:

Actions taken by The Alight Investigations Team

Identify the actions that Alight took in response to the incident:

- A freeze was placed on the account and an investigation was initiated.
- Account access was reviewed, preserved, and summarized including transactions, bank account and routing data, recorded telephone calls, account changes, public record searches, and other relevant information.
- An internal search was performed of other customers who could have been affected by the known data points found during the investigation. No additional matches were found.
- Once Alight's Fraud Protection Team confirms the activity in the account was not conducted by the customer, the client team will seek to recoup taxes withheld for the total distribution and have those funds placed back into the customer's account.
- A summary of the investigation along with talking points for identity theft and law enforcement involvement will be provided to the customer (Appendix A).

Appendix A: Customer Recommendations

- We appreciate your patience as we've worked through our investigation. I want to update you on the status of our findings.
- On 9/14/20, a representative from Colgate-Palmolive contacted Alight and reported they suspected your 401k account had a fraudulent distribution that occurred on 3/17/20.
- Once the information as reported to us, we escalated the issue to our Fraud Protection Team, placed a freeze on your account, and requested our Investigations Team look into the issue.
- Our Investigations Team reviewed your account and found:
 - Beginning on 1/29/20, a bad actor contacted the Customer Care Center by telephone and impersonated you. During the interaction, the caller provided your full name, last 4 of SSN, date of birth, and current address on file in South Africa. The caller requested a Phone PIN reset. A Temporary Phone PIN was sent to the address we had on file in South Africa and about three weeks later it was entered into Alight's Automated Phone System and a permanent Phone PIN was chosen.
 - Over the next several months, a bad actor continued to impersonate you via calls to the Customer Care Center and via web activity within your account. This included adding an email address, international telephone number, bank account for direct deposit, and a new permanent address in Las Vegas, NV. In each instance, calls to the Customer Care Center were properly secured with the Phone PIN. Web sessions were properly authenticated and occurred from IP addresses in South Africa.
 - On 3/17/20, the bad actor contacted the Customer Care Center, secured the call by Phone PIN, and requested a total distribution from your 401k to be paid by check to an address on file for your account in Las Vegas, NV. The distribution was processed for \$751,430.53 gross (\$601,144.42 net). The net amount included withholdings for taxes. A check made payable to your name was sent for the net amount and cashed on 3/27/20. We obtained a copy of the endorsed check as part of our investigation.
- After the account changes were made and distribution was requested, we sent notifications to you by a variety of methods including postal mail and email.
- If you did not conduct this transaction, we will file a claim and attempt to recoup the tax withholdings to return to your account.
- You should contact law enforcement and file a police report for identity theft and 401k theft. Please provide us with the agency name, report number, and officer name. We do not have any more information about specifically who the third party was who accessed your account, but we'll contact the law enforcement agency and offer to provide any information we have. We will fully cooperate with their investigation and help in any way we can.

- You can also contact the Federal Trade Commission to report any incidents of identity theft or to receive additional guidance on steps you can take to protect against identity theft.
- We recommend you change your benefits account User ID, Password, and Security Questions.
- We recommend you check your other personal accounts and change those passwords.
- You might consider purchasing identity theft monitoring since some personal information may have been compromised. You can find more information about how to recover from identity theft by visiting the U.S. Government website (www.identitytheft.gov).
- To protect your credit, contact one of the three major credit bureaus to place a fraud alert. A fraud alert will prevent new credit accounts from being opened.
 - Equifax: 1.800.525.6285 or www.equifax.com
 - Experian: 1.888.397.3742 or www.experian.com
 - TransUnion: 1.800.680.7289 or www.transunion.com
- We have general suggestions to keep your account safe.
 - We recommend you keep the contact information in your benefits account up-to-date in case we need to get in touch with you.
 - Please review your benefits account regularly and report any suspicious activity to us promptly.
 - When you create a Password for your benefits account, please create one that is strong and unique. Do not reuse a Password that is also used for other web logins or online accounts you might have. Do not share your User ID and Password with anyone.
 - Please protect your digital devices by installing anti-virus software and keep your operating systems, web browser, and applications up to date with the latest updates from these providers.
 - Please avoid clicking on suspicious emails or links within suspicious emails or text messages. These are often known as “phishing” attempts and sometimes can include can language asking you to act quickly or provide some of your personal identifying information like your Social Security Number, Date of Birth, or Passwords. These are some methods that people use to trick you and steal your identity or personal information.